Hive0117 Continues Fileless Malware Delivery in Eastern Europe

securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/

Malware April 26, 2022

By Melissa Frydrych co-authored by Claire Zaboeva , David Bryant 4 min read

Through continued research into the ongoing cyber activity throughout Eastern Europe, IBM Security X-Force identified a phishing email campaign by Hive0117, likely a financially motivated cybercriminal group, from February 2022, designed to deliver the fileless malware variant dubbed DarkWatchman. The campaign masquerades as official communications from the Russian Government's Federal Bailiffs Service, the Russian-language emails are addressed to users in Lithuania, Estonia, and Russia in the Telecommunications, Electronic and Industrial sectors. The activity predates and is not believed to be associated with the Russian-led invasion of Ukraine.

X-Force assesses that it is possible the targeting of telecommunication providers and their industry adjacent suppliers may be intended as ultimately serving to enable illegal access to numerous distributed clients and end-users.

DarkWatchman is a malicious Remote Access Trojan (RAT) based on JavaScript, using command and control (C2) mechanisms for fileless persistence, as well as other capabilities.

The phishing activity discovered by X-Force (tracked internally as Hive0117) aligns with research published in December 2021, detailing a similar phishing campaign designed to deliver a DarkWatchman payload by imitating a Russia-based freight and logistics company.

Given the elevated levels of threat activity associated with the ongoing regional crisis, the evidence may suggest that threat actors will leverage the current climate to conduct and obfuscate further activity.

Hive0117 Activity Assessment

X-Force assesses Hive0117 phishing campaigns are likely criminally motivated in nature given the target selection and focuses of current and previous activities. Additionally, while the target list of the phishing campaign attributed to Hive0117 has regional associations with the Russian invasion of Ukraine, the activity predates the invasion, indicating the separate from any politically charged associations that have spurred recent waves of criminal activity, such as the attack on a German subsidiary of a Russian state-affiliated energy company.

Nevertheless, given the evolving nature of criminal activity prompted by the conflict, language capability, target focus, and relative sophistication of the actor, it is likely Hive0117-related activity possesses an elevated threat to entities and enterprises based in-region.

Hive0117 Phishing Activity

X-Force discovered multiple emails that were sent in mid-February 2022 to individual users, including a state-owned communication company based in Lithuania, a prominent Industrial Enterprise in Estonia, and several electronic and telecommunication businesses located in Russia. In some cases, the emails were targeting company owners, as well as individuals in

leadership positions associated with Dispatch Services and Sales. Targeted organizations could be of high value to criminal actors given the targets' potential trusted access to wide, and distributed client base.

The emails are crafted to appear to originate from the official address of the Federal Bailiffs Service in Russia, a federal law enforcement agency under the Russian Ministry of Justice; however, header examination revealed that some of the emails were received from shtampuy[.]ru (free.ds [185.64.76.158]). The majority of emails feature the return path address [.]fssprus[.]ru, meant to imitate the organization's authentic address https://r77.fssp.gov[.]ru. However, for unknown reasons, a single instance imitates a sender which seeks to pose as the head of a purported Russian investment company. The subjects of Hive0117 emails, including official notices, are eye-catching and are likely intended to compel the target to open the email and access the attachment.

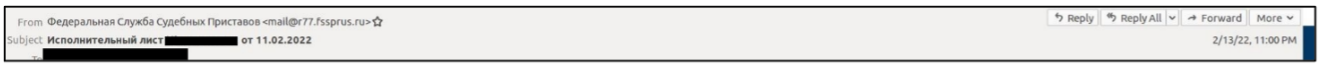

Image 1: Sample of email return path and subject line

The contents of the emails feature identical Russian-language text detailing several articles related to enforcement procedures associated with the Kuntsevsky District Court of Moscow, upheld by the "Bailiff of the Interdistrict Department of Bailiffs for the Execution of Decisions of the Tax Authorities." The only variation observed by X-Force within the emails is in the name and "case number" associated with the individual email and accompanying malicious ZIP archive file attachment.

Image 2: Sample email body

X-Force assesses that it is possible the targeting of telecommunication providers and their industry adjacent suppliers may be intended as ultimately serving to enable illegal access to numerous distributed clients and end-users.

Malware Payload

The emails X-Force uncovered contain archive files either named “Исполнительный лист XXXXXXX-22.zip”, where the “X” indicates a numeric value, or “Счет 63711-21 от 30.12.2021.zip”, translated respectively to “Performance List”, “Writ of Execution”, and “Invoice”. Each archive file contains an executable of the same name, designed to deliver the DarkWatchman JavaScript backdoor and encrypted source code for a keylogger similarly to the report from December 2021.

In addition, X-Force discovered downloader files designed to deliver the DarkWatchman malware, by contacting domtut[.]site|fun|online and downloading files to %TEMP%. Un execution a self-extracting archive (SFX) installer drops two files: a Javascript (JS) file and a file containing a series of hexadecimal characters. The JS file contains obfuscated code that functions as the backdoor and the hexadecimal data contains encrypted data that when decrypted, contains a block of base64 encoded PowerShell that executes a keylogger. The configuration contains a comment in Russian text, which translates to “The comment below contains SFX script commands” (;Расположенный ниже комментарий содержит команды SFX-сценария), indicating that the author of the malware is a Russian-language speaker, possibly based in, or originating from, a Russian-speaking territory.

Given the fileless nature of the malware, coupled with a JavaScript and a keylogger written in C#, and the abilities to remove traces of its existence on the compromised system when instructed, X-Force assesses that malicious actor(s) behind Hive0117 activity are of moderate sophistication.

Malware Infrastructure

The majority of the new malware samples discovered by X-Force, appear to be based on a C2 IP address (103.153.157[.]33) previously associated with Hive0117 activity. One of the samples was submitted to Virus Total in February 2022 and is configured to use several C2 domains including d303790c[.]top, which overlaps with previously uncovered malicious executable Накладная №12-6317-3621.exe.

The DarkWatchman malware analyzed by X-Force uses a domain generation algorithm (DGA) to generate a list of C2 domains, in which the malware attempts to communicate with. The DGA requires a salt as input stored in the configuration key *b*, or the default salt *d46ebd15* is used if the key is not set. A list of hard-coded domain strings is contained in an array, with the analyzed samples containing the following list:

3a60dc39, 4d67ecaf, d303790c, a404499a, 3d0d1820, 4a0a28b6, dab53527, adb205b1, 44e645b3, 500ed27c, c8690767, 17c45148, 13e1ced9, e123fe80, 136e9446, 5937c7c6, 7c7cb9a4, 9eaa332e, 97815a39, 6a090054

IOCs

Files

File Name	Hash
Исполнительный лист 1840120-22.exe	d68180819bb8eb8207dc6ab74c1a4642
Исполнительный лист 1909102-22.exe	2bd8ee514c13a06687b5775e0a9eaf71
Исполнительный лист 16301123-22.exe	b25b24998800da7b5cf17879f2eb83ed
Исполнительный лист 1711390-22.exe	79b824bb99b4cc4f5da880371de52977
Исполнительный лист 154211671.scr	a4f19fba9a5ec97d3560cd43c4bd5507
Исполнительный лист 154211671.scr	a34809f26a22e0127e99597fed9169bf
Счет 63711-21 от 30.12.2021.exe	75a3b83d2b4131132d76d92190f045ec

Domains

3a60dc39[.]\(top|fun|online|site)
4d67ecaf[.]\(top|fun|online|site)
d303790c[.]\(top|fun|online|site)
a404499a[.]\(top|fun|online|site)
3d0d1820[.]\(top|fun|online|site)
4a0a28b6[.]\(top|fun|online|site)
dab53527[.]\(top|fun|online|site)
adb205b1[.]\(top|fun|online|site)
44e645b3[.]\(top|fun|online|site)
500ed27c[.]\(top|fun|online|site)
c8690767[.]\(top|fun|online|site)
17c45148[.]\(top|fun|online|site)
13e1ced9[.]\(top|fun|online|site)
e123fe80[.]\(top|fun|online|site)
136e9446[.]\(top|fun|online|site)
5937c7c6[.]\(top|fun|online|site)
7c7cb9a4[.]\(top|fun|online|site)
9eaa332e[.]\(top|fun|online|site)
97815a39[.]\(top|fun|online|site)
6a090054[.]\(top|fun|online|site)

URLs

http[:]//domtut[.]\(fun|online|site)

IP Addresses

103.153.157.33

Melissa Frydrych
Threat Hunt Researcher, IBM

Melissa is an analyst on the Threat Hunt & Discovery Team within IBM X-Force. She has over 9 years of experience, investigating and analyzing cyber threa...


IBM Security